



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,161	05/16/2005	Kaisa Nyberg	59643.00600	6511
32294 7590 04/28/2009 SQUIRE, SANDERS & DEMPSEY L.L.P. 8000 TOWERS CRESCENT DRIVE 14TH FLOOR VIENNA, VA 22182-6212				
EXAMINER				
ABYANEH, ALI S				
ART UNIT		PAPER NUMBER		
2437				
MAIL DATE		DELIVERY MODE		
04/28/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/528,161

Applicant(s)

NYBERG ET AL.

Examiner

ALI S. ABYANEH

Art Unit

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 January 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10, 13-20 and 23-69 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10, 13-20, and 23-69 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 March 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-10, 13-20, and 23-69 are amended.
are presented for examination.
2. Claims 1-5, 8, 10, 13-15 and 17-20 are amended.
3. Claims 11, 12, 21 and 22 are cancelled.
4. Claims 23-69 are newly added.
5. Examiner withdraws the objection to the specification (abstract) due to the correction by the applicant.
6. Examiner withdraws the objection to the claims 18-20 due to the correction by the applicant.
7. Examiner withdraws the 101 rejection of claim 18 due to the correction by the applicant.

Response to Arguments

8. Applicant's amendments/arguments filed on 01-07-2009 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claim 2, 23, 28, 49 and 59 are rejected under 35 U.S.C. 112, second paragraph, for the following reasons:

Claim 2, 28, 38, 49 and 59 recites the limitation "the authentication functionality".

Claim 13 recites the limitation "the input data".

There are insufficient antecedent basis for these limitations in the claims.

Claim 23 in line 4 recites the limitation "sharing between authentication functionality and the challenge data". It is not clear as what is being shared/sharing between authentication functionality and the challenge data.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1-7, 14-20, 23-28, 33-38, 43-49, 54-59 and 64-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Young et al. (US Patent No. 7,350,076) in view of McGarvey (US Patent No. 7,287,156).

Regarding claim 1 and 67

Young teaches a method, comprising: executing an authentication protocol, wherein the terminal authentication protocol comprise authenticating an

identity of a network entity by a terminal in a communication system; sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity (column 10, lines 38-53); and

sharing challenge data between the network entity and the terminal; forming at the terminal test data by applying an authentication function to the challenge data; sending a message comprising terminal authentication data, from the terminal to the network entity (column 11, lines 10-17); and determining, based on the terminal authentication data, whether to provide the terminal with access to the service, wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key (column 11, lines 18-30).

Although Young teaches "the second device is authenticated to the first device using a conventional authentication protocol" he does not explicitly teach executing a second protocol in addition to the previous protocol. However, in an analogous art, McGarvey teaches executing another protocol (column 2, lines 20-24).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Young to include executing another protocol. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated do so in

order to provide authentication of messages where a principal and a resource utilize different security protocols (column 1, lines 9-11).

Regarding claim 18

Young teaches a system: comprising: a terminal configured to apply authentication functions to input data to form response data; and a network entity configured to provide access to a service, wherein the system is configured to perform an authentication method of executing an authentication protocol, wherein the authentication protocol comprises authenticating an identity of the network entity by the terminal in the system; sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity (column 10, lines 38-53); and sharing challenge data between the network entity and the terminal; forming at the terminal test data by applying an authentication function to the challenge data; sending a message comprising terminal authentication data from the terminal to the network entity (column 11, lines 10-17); and determining, based on the terminal authentication data, whether to provide the terminal with access to a service; wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key (column 11, lines 18-30).

Although Young teaches "the second device is authenticated to the first device using a conventional authentication protocol" he does not explicitly teach executing a second protocol in addition to the pervious protocol. However, in an analogous art, McGarvey teaches executing another protocol (column 2, lines 20-24).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Young to include executing another protocol. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated do so in order to provide authentication of messages where a principal and a resource utilize different security protocols (column 1, lines 9-11).

Regarding claim 26, 47 and 68

Young teaches a method, comprising: executing an authentication protocol, wherein the authentication protocol comprises authenticating an identity of a network entity by a terminal in a communication system, and receiving a key at the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity (column 11, lines 10-17); and receiving challenge data from the network entity at the terminal; forming at the terminal test data by applying an authentication function to the challenge data; sending a message comprising terminal authentication data from the terminal to the network entity (column 11, lines 10-17); and receiving access

to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the terminal key (column 11, lines 18-30).

Although Young teaches "the second device is authenticated to the first device using a conventional authentication protocol" he does not explicitly teach executing a second protocol in addition to the previous protocol. However, in an analogous art, McGarvey teaches executing another protocol (column 2, lines 20-24).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Young to include executing another protocol. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated do so in order to provide authentication of messages where a principal and a resource utilize different security protocols (column 1, lines 9-11).

Regarding claim 36, 57 and 69

Young teaches a method, comprising: executing an authentication protocol, wherein the authentication protocol comprises sending an identity of a network entity for authentication by a terminal in a communication system; sending a key to the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity (column 11, lines 10-17); and sending challenge data from the network entity to

the terminal for forming test data at the terminal by applying an authentication function to the challenge data; receiving a message comprising terminal authentication data from the terminal at the network entity (column 11, lines 10-17); determining, based on the terminal authentication data, whether to provide the terminal with access to a service; and providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key(column 11, lines 18-30).

Although Young teaches "the second device is authenticated to the first device using a conventional authentication protocol" he does not explicitly teach executing a second protocol in addition to the pervious protocol. However, in an analogous art, McGarvey teaches executing another protocol (column 2, lines 20-24).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Young to include executing another protocol. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated do so in order to provide authentication of messages where a principal and a resource utilize different security protocols (column 1, lines 9-11).

Regarding claim 2

Young furthermore teaches a method further comprising: forming the test data by applying the authentication function to the challenge data at the

authentication functionality; and sending the test data from the authentication functionality to the network entity, wherein the determining comprises forming network authentication data by applying the predetermined function to the test data and the key at the network entity (column 11, lines 10-17), and wherein the determining further comprises providing the terminal with access to the service only when the terminal authentication data equals the network authentication data (column 11, lines 18-30).

Regarding claim 3

Young furthermore teaches sending the key from the network entity to the authentication functionality; forming the test data by applying the authentication function to the challenge data at the authentication functionality; and forming network authentication data by applying the predetermined function to the test data and the key at the authentication functionality (column 11, lines 18-30).

Regarding claim 4

Young furthermore teaches a method, comprising: sending the terminal authentication data from the network entity to the authentication functionality; and sending from the authentication functionality to the network entity an indication of whether the terminal authentication data equals the network authentication data,

wherein the determining comprises providing the terminal with access to the service only when the indication is that the terminal authentication data equals the network authentication data (column 11, lines 18-30).

Regarding claim 5

Young furthermore teaches a method, comprising: sending the network authentication data from the authentication functionality to the network entity, wherein the determining comprises providing the terminal with access to the service only when the indication is that the terminal authentication data equals the network authentication data (column 11, lines 17-27).

Regarding claim 6, 27, 37, 48 and 58

Young furthermore teaches a method, wherein the terminal authentication data is formed as a cryptographic checksum (column 11, lines 20-22).

Regarding claim 7, 28, 38, 49 and 59

Young furthermore teaches a method, wherein the network entity is co-located with the authentication functionality (column 9, lines 34-55).

Regarding claim 14, 15, 33, 34, 43, 44, 54, 55, 64 and 65

Young furthermore teaches wherein the authentication protocol is the one of a pre-internet key exchange credential provisioning protocol, a protected

extensible authentication protocol, or an extensible authentication protocol-tunneled transport layer security; wherein the challenge data and the response data are formed according to the extensible authentication protocol (column 12, lines 14-19).

Regarding claim 16, 35, 45, 56 and 66

Young furthermore teaches a method, wherein the said message is a dedicated authentication message (column 11, lines 10-17).

Regarding claim 17, 46

Young furthermore teaches a method, wherein the predetermined function is used for derivation of a session key to be used for encryption and/or authentication of communications between the terminal and the network entity (column 10, lines 13-16).

Regarding claim 19

Young furthermore teaches wherein the system is further configured to execute a linking protocol by forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol, and forming at the network entity secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol,

wherein the secret session keys are configured to secure the subsequent communications between the terminal and some network element (column 11, lines 3-9).

Regarding claim 20

Young furthermore teaches forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol; and forming at the network entity secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol, wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element (column 11, lines 3-9).

Regarding claim 23

Young furthermore teaches executing a third authentication protocol for authentication of the terminal comprising: sharing between an authentication functionality and the challenge data; forming response data and another key at the terminal by applying the authentication function to the challenge data; sending the response data to the authentication functionality from the terminal;

authenticating the terminal at the authentication functionality using the response data; and applying the authentication function to the challenge data to duplicate the another key (column 11, lines 10-17).

Regarding claim 24

Young furthermore teaches a method wherein the third authentication protocol is an authentication and key agreement protocol or any protocol of the extensible authentication protocol family (column 12, lines 14-19).

Regarding claim 25

Young furthermore teaches a method wherein the test data comprises one or both of an authentication and key agreement protocol integrity key value or an authentication and key agreement protocol cipher key value (column 11, lines 12-17).

13. Claims 8-10, 13, 29-32, 39-42, 50-53, 60-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Young et al. (US Patent No. 7,350,076) in view of McGarvey (US Patent No. 7,287,156) further in view of Ala-Laurila et al. (US Patent No. 7,356,145).

Regarding claim 8, 29, 39, 50 and 60

Young and McGarvey teach all limitation of the claim as applied to claim 1, 26, 36, 47 and 57 above. Young and McGarvey do not explicitly teach wherein an identity module of the terminal is configured to perform the authentication function. However, in an analogous art, Ala-Laurila teaches an identity module of the terminal is configured to perform the authentication function (column 3, lines 27-30).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Young and McGarvey to include an identity module of the terminal is performing the authentication function. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated do so since identity modules are well known and are widely used in the art for performing authentication.

Regarding claim 9, 10, 13, 30-32, 40-42, 51-53 and 61-63

Ala-Laurila furthermore teaches wherein the identity module is user-removable from the terminal, wherein the identity module is a subscriber identity module or a universal subscriber identity module; and wherein the identity module is configured to store a code and the authentication function comprises cryptographic transformation applied to the code and the input data (column 3, lines 10-30).

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/A. S. A./

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437